APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: NEW COMMUNICATION TECHNIQUES FOR SIMPLE NETWORK MANAGEMENT PROTOCOL

APPLICANT: ALEX O. AGERHOLM AND KELL MICHAEL JENSEN

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL688267890US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C 20231.

November 30, 2000
Date of Deposit

Signature

Rich Donovan
Typed or Printed Name of Person Signing Certificate

NEW COMMUNICATION TECHNIQUES FOR SIMPLE NETWORK MANAGEMENT PROTOCOL

BACKGROUND

Simple network management protocol or SNMP is described in various RFCs, including SNMP v1 described in re RFC1155, Internet Engineering Task Force (IETF), 1997 and other flavors of SNMP including v2 and v3. SNMP can be used to exchange data between computers that indicates about network activity. The data travels between a number of managed computers/nodes and a network management station. A number of different network devices such as sub agents, master agents, and the like may also be managed using the SNMP protocol. The details of SNMP communications are well known in the art. The communications may produce a file, such as a MIPS file, that includes a textual data describing the network. The system often uses a polled interface which sends information to every item on the network, and receives information back.

SNMP is used by existing computer programs such as HP OpenView ™.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects will now be described with reference to the accompanying drawings, in which:

Figure 1 shows a basic SNMP managed network;

Figure 2 shows a basic diagram of how the SNMP is encapsulated into HTTP;

Figure 3A and 3B shows a flow diagram of the SNMP request through HTTP via the network and

Figure 4 shows encapsulating SNMP protocol into secure HTTP.

DETAILED DESCRIPTION

Figure 1 shows a basic network of the type contemplated according to the present system. A number of computers 100, 105, 110 are interconnected to one another over an intranet type network connection 99. One of these computers, here 100, is designated as the master, or in SNMP protocol, the network management system. The intranet 99 may also be connected to network components outside of the intranet 99 through an Internet 115. Such a connection is conventionally carried out via a firewall 120. The firewall 120 attempts to intercept and block all undesired or unknown traffic. Only information having certain

characteristics is allowed to pass the firewall 120.

The internet may be the publicly-available "Internet", or a private gateway of any type, such as a dial-in gateway.

Parts of the network, such as computers 130 and 135, may be located on the Internet connection 115 and hence outside the firewall. However, a message that is in SNMP protocol may not be able to pass the firewall to monitor these computers. At the very least, a custom change of the firewall may be necessary. Moreover, in SNMP protocol version 3, a special socket called UDP is run which may make it difficult to set up the firewall for passage of SNMP protocol, even if this were desired.

This invention recognizes that virtually every firewall is configured to pass HTTP Internet traffic. Since the HTTP traffic can traverse the firewall, the present system defines encapsulating the SNMP Traffic into the HTTP Protocol. Figure 2 shows the conceptual layout. The server 100 is shown on one side of the firewall 120. One of the managed devices 130 is shown on the other side of the firewall. The device to manage 130 creates SNMP information 200 which is basically textual information. Textual information is written as text within an HTTP sequence 205. All aspects of the sequence are interpreted

as HTTP. The HTTP protocol is then formed into an Internet protocol, and sent via the MAC layer to 15 to the Internet connection 115. The firewall 120 sees an HTTP protocol. Since HTTP traffic is almost always allowed through firewalls, the SNMP protocol is allowed to pass through the firewall 120 and is received by the management station 100.

A more detailed flow diagram is shown in figures 3A and 3B. Figure 3A shows the management station sending the SNMP request. The SNMP request 300 is built as an HTTP sequence including the SNMP request. The text of the HTTP message can be, for example, GET SNMP://1.4.7.9.2.3 where the latter numbers are the numbers representing the managed device whose information is desired. At 310, the HTTP message is sent over the Internet connection 115 through the firewall 120. At 315, the managed station 130 receives the request, and removes the encapsulation at 320. This can produce the original text from the SNMP message. The SNMP request is therefore received at 325 by the standard SNMP program that monitors the requests.

Figure 3B shows the SNMP program acting on the request received at 325 to produce a response. From the point of you of the SNMP program, this is a normal request in SNMP protocol. The response is sent to an encapsulator which at 335 builds an HTTP response including the SNMP response. A

sample SNMP response would be as follows:

<SNMP>

OID=1.4.7.9.2.3

Value="Running"

<\SNMP>

Note that this includes taqs <SNMP>, <\SNMP>which look like HTTP tags. These tags can be defined in a specific version of the HTTP, or else most browsers will interpret them as unknown tags and simply ignore the text in between them. However, since the SNMP information will likely never be read by a browser, defining these may be unnecessary. In any case, this sequence is sent as though it were an HTTP response at 340. Again, this is put onto the Internet connection 115, and passes the firewall 120 to be sent to the management station 100. Management station 100 receives the HTTP sequence at 345, and removes the encapsulation at 350. Once the encapsulation is removed, the SNMP response is handled at 355 exactly like any normal SNMP response would be handled.

Significant advantages of this system can be expected. Since the SNMP program can operate as normal, this system may be totally transparent to the SNMP program. In another embodiment, however, it may be the SNMP program itself that does the HTTP encapsulation.

In another embodiment, shown in figure 4, the SNMP protocol is encapsulated using secure HTTP or HTTPs protocol. This provides a secure socket link (SSL) to the session, thereby providing security on the protocol. SSL can provide much higher security then any version of the SNMP. For example, the newest version of the SNMP V3 provides a maximum 56 bit key. HTTP can easily provide a 128 bit key.

This system can run in software on a computer as described herein, and also can run in hardware such as a field programmable gate array, digital signal processor or other hardware device.

In addition, while this system has been described for use with SNMP, this same technique can be used with other management schemes which have a message which will not pass a firewall. In any of these management schemes, the actual data can be encapsulated into HTTP and used to control the firewall.

Although only a few embodiments have been disclosed in detail above, other modifications are possible. All such modifications are intended to be encompassed within the following claims.